UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,881	03/15/2005	Masahiro Wakamori	MAT-8676US	2252

23122 7590 01/29/2008

RATNERPRESTIA
P O BOX 980
VALLEY FORGE, PA 19482-0980

EXAMINER	
PACHURA, REBECCA L	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
01/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/527,881	WAKAMORI ET AL.	
	Examiner	Art Unit	
	Rebecca L. Pachura	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03/15/2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :03/15/2005, 01/20/2006, 03/31/2006, 08/03/2006.

DETAILED ACTION

1. **Claims 1-20 are presented for examination.**

The claims and only the claims form the metes and bounds of the invention. "Office personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969)" (MPEP p 2100-8, c 2, l 45-48; p 2100-9, c 1, l 1-4). The Examiner has full latitude to interpret each claim in the broadest reasonable sense. The Examiner will reference prior art using terminology familiar to one of ordinary skill in the art. Such an approach is broad in concept and can be either explicit or implicit in meaning.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 08/03/2006, 03/31/2006, 01/20/2006, and 03/15/2005 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Preliminary Amendment

3. The preliminary amendments of the Title, Specification, Claims, and Drawings submitted on 03/15/2005 are duly noted.

Priority

4. The foreign priority claim filed on 07/11/2003 #2003-273315 in Japan is duly noted.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. **Claims 12 and 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**

Claims 12 and 20 recites the limitation "*the authenticatee*" in lines 2 and 4. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. **Claims 1, 2, and 4 are rejected under 35 U.S.C. 102(b) as being anticipated by US 5280527 (Gullman) (Applicant's IDS).**

As to claim 1, Gullman discloses an authentication system comprising: an authenticator including: an authentication processor to authenticate whether or not an authenticatee is a user previously registered (Gullman column 2, lines 27-37: According to one aspect of the invention, the biometric security mechanism stores a template of user biometric information (i.e., signature, finger-print, voice-print). To access the host system, the user enters the corresponding biometric information to the security mechanism. The mechanism verifies the input against the template, then generates and displays a token based on the verification. The user then communicates the token to the host system which decodes the token and determines whether access is authorized);

and a data output part to output an identification data when the authenticatee is authenticated as the user previously registered (Gullman column 2, lines 33-35: The mechanism verifies the input against the template, then generates and displays a token based on the verification); and

a server including: a credit appraiser to appraise credit of the authenticatee according to the identification data output from the data output part; and an appraisal result output part to output a result in the credit appraiser (Gullman column 4, lines 13-36: The access device 12 sends the token to the host 10 which decodes the token to identify the embedded fixed code and correlation factor. In an alternative embodiment, the security apparatus 14 is coupled directly to the host system 10, such that the token output is transmitted directly to the host without the need for displaying the token or manual entry by the user. The coupling can be accomplished using, for example, standard data communication cable or any other known data transmission technique. To properly decode the token, the security apparatus 14 is synchronized with the host system 10 so that the time varying code is identical at both the security mechanism 14 and the host system 10. In the challenge code embodiment, the host system, having generated the challenge code, retains the challenge code in memory to decode the token. The host 10 identifies the user with the fixed code and verifies the identification based on the correlation factor. The host system 10 permits full or limited entry based upon the level of authorization assigned to a given user (as identified by the fixed code). For example, a given user may be allowed to perform an electronic funds transfer only from a prescribed account).

As to claim 2, Gullman discloses the authentication system of claim 1, wherein the authenticator includes an image reader to input an image data, and the authentication processor

authenticates the authenticatee according to the image data input from the image reader (Gullman column 5, lines 42-55: The biometric sensor 18 detects biometric input from a user (i.e., card-holder, pen-holder), the exact nature of which is not critical to the invention, so long as it senses information which is basically personal and substantially invariant in characteristics which are detected. According to various embodiments, the sensor 18 may detect a fingerprint, a signature, a voice or other like information. For the card embodiment 14', the sensor 18 may be a scanning device which detects a fingerprint or pressure sensing device which detects a signature. Alternatively, a CCD imaging device could be used to capture a picture of the fingerprint or signature. The sensor 18 also could be a voice detector).

As to claim 4, Gullman discloses the authentication system of claim 1, further comprising a terminal comprising a terminal including an appraisal result input part to input the appraisal result output from the server (Gullman column 3, lines 37-39: According to the invention, the biometric security mechanism 14 generates a security token which the user inputs to the access device).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 3 and 5-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5280527 (Gullman) (Applicant's IDS) as applied to claim 1 above, in view of EP 1081662 A2 (Takizawa) (Applicant's IDS), and in view of US 20020194137 (Park).**

As to claim 3, Gullman discloses the authentication system of claim 2. Gullman fails to teach wherein an eye-image of the authenticatee is used as the input image data and the authentication processor includes: an authentication data producer to produce an authentication data according to an iris pattern of the eye image of the authenticatee; a storage to store a login authentication data; and a collator to collate the login authentication data with the authentication data produced according to the eye image.

However, Takizawa discloses wherein an eye-image of the authenticatee is used as the input image data and the authentication processor includes: an authentication data producer to produce an authentication data according to an iris pattern of the eye image of the authenticatee (Takizawa abstract); a storage to store a login authentication data (Takizawa column 7, paragraph 0053: ...The transferred data is stored in the database in the iris certificate authority...); and a collator to collate the login authentication data with the authentication data produced according to the eye image (Takizawa column 8, paragraph 0055: ...The database contains the name, address, ID, iris data of each customer and his authentication code formed by adding an electric signature to the certificate....).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Gullman and Takizawa because Gullman teaches using biometric information to authenticate a user and Takizawa teaches using iris scanning (which is biometric

information) to authenticate a user (Takizawa abstract, column 7, paragraph 0053: ...The transferred data is stored in the database in the iris certificate authority...and column 8, paragraph 0055: ...The database contains the name, address, ID, iris data of each customer and his authentication code formed by adding an electric signature to the certificate....).

As to claim 5, the modified Gullman discloses the authentication system of claim 4. The modified Gullman fails to teach wherein the authenticator has a data input part to input a data including a data on a product to be transacted, and the terminal has a data output part to output a data including a data on the product to be transacted to the data input part of the authenticator.

However, Takizawa discloses wherein the authenticator has a data input part to input a data including a data on a product to be transacted, and the terminal has a data output part to output a data including a data on the product to be transacted to the data input part of the authenticator (Takizawa column 8, paragraph 0059: ...the POS installed in the shop sums up purchase prices input at purchases of articles, and displays a total sum of money).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Gullman and Takizawa because they both teach authenticating for monetary transactions (Takizawa column 8, paragraph 0059: ...the POS installed in the shop sums up purchase prices input at purchases of articles, and displays a total sum of money... and Gullman column 4, lines 34-36: For example, a given user may be allowed to perform an electronic funds transfer only from a prescribed account).

As to claim 6, Gullman discloses an authentication system comprising: a server including. Gullman fails to teach a storage to store a login authentication data of a user to be registered.

However, Takizawa discloses a storage to store a login authentication data of a user to be registered (Takizawa column 7, paragraph 0053: ...The transferred data is stored in the database in the iris certificate authority...).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that a means to store login authentication data would be necessary in order to compare what is registered with what the user is inputting (Takizawa column 7, paragraph 0053: ...The transferred data is stored in the database in the iris certificate authority...).

Gullman discloses and an authentication processor to execute a predetermined authentication process (Gullman column 2, lines 27-37: According to one aspect of the invention, the biometric security mechanism stores a template of user biometric information (i.e., signature, finger-print, voice-print); and a data output part to output the login authentication data and the authentication processor (Gullman column 2, lines 33-35: The mechanism verifies the input against the template, then generates and displays a token based on the verification); and an authenticator including: an authentication data input part to input an authentication data of an authenticatee (Gullman column 4, lines 40-45: ... The apparatus 14 includes a power source 15, on/off switch 16, biometric sensor 18, display 20, processor 22 with on-chip random access memory, biometric input section 33 for receiving biometric information from the biometric sensor a read only memory...); an data input part to input the login authentication data and the

authentication processor (Gullman column 2, lines 40-47: According to another embodiment of the invention, the token is derived from the results of the above described biometric comparison, plus a user input challenge code from the host, rather than a time varying value. In a further embodiment, the biometric information is collected from the operation of the user of inputting the challenge to the device, either using a keypad, writing tablet or by voice...); and a processor to perform a predetermined processing using the authentication data (Gullman column 2, lines 53-57: ... Upon entry of the cardholder's biometric information, the processor executes the verification algorithm. The verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN, embedded serial number, account number...)), wherein the authenticator reads the authentication processor input from the server into the processor to collate the authentication data of the authenticatee with the login authentication data of the authenticatee using the authentication processor read into the processor (Gullman column 2, lines 40-47: According to another embodiment of the invention, the token is derived from the results of the above described biometric comparison, plus a user input challenge code from the host, rather than a time varying value. In a further embodiment, the biometric information is collected from the operation of the user of inputting the challenge to the device, either using a keypad, writing tablet or by voice...).

As to claim 7, the modified Gullman discloses the authentication system of claim 6. The modified Gullman fails to teach further comprising a register having a login authentication data input part to input a login authentication data of the user to be registered and a login authentication data output part to output the login authentication data.

However, Takizawa discloses further comprising a register having a login authentication data input part to input a login authentication data of the user to be registered and a login authentication data output part to output the login authentication data (Takizawa Figure 1 and column 5, paragraph 0021: The electronic payment system according to the present invention comprises an iris registration device...).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that it would be necessary to have the ability to input and output the information the user registered (Takizawa Figure 1 and column 5, paragraph 0021: The electronic payment system according to the present invention comprises an iris registration device...).

The further modified Gullman discloses wherein the server includes a data input part to input the login authentication data and the authentication processor (Gullman column 2, lines 40-47: According to another embodiment of the invention, the token is derived from the results of the above described biometric comparison, plus a user input challenge code from the host, rather than a time varying value. In a further embodiment, the biometric information is collected from the operation of the user of inputting the challenge to the device, either using a keypad, writing tablet or by voice...). The further modified Gullman fails to teach the register outputs the login authentication data input into the login authentication input part from the data output part to the data input part of the server.

However, Takizawa discloses the register outputs the login authentication data input into the login authentication input part from the data output part to the data input part of the server

(Takizawa Figure 1 and column 5, paragraph 0021: The electronic payment system according to the present invention comprises an iris registration device...).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that it would be necessary to have the ability to input and output the information the user registered (Takizawa Figure 1 and column 5, paragraph 0021: The electronic payment system according to the present invention comprises an iris registration device...). The further modified Gullman fails to teach and the server stores the login authentication data input into the data input part in the storage.

However, Takizawa discloses and the server stores the login authentication data input into the data input part in the storage (Takizawa column 7, paragraph 0053: ...The transferred data is stored in the database in the iris certificate authority...).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that a means to store login authentication data would be necessary in order to compare what is registered with what the user is inputting (Takizawa column 7, paragraph 0053: ...The transferred data is stored in the database in the iris certificate authority...).

As to claim 8, the modified Gullman discloses the authentication system of claim 6, wherein the server includes an encrypter to encrypt the authentication processor and the login authentication data by a predetermined encrypting method; stores a decrypter to decrypt encrypted the authentication processor and the login authentication data in the storage; and outputs the decrypter and encrypted the authentication processor and the login authentication data; and the authenticator decrypts the authentication processor and the login authentication data

input into the data input part by the decrypter (Gullman column 5, lines 15-33: Alternatively, processor 20 may include a standard encryption module which applies an encryption algorithm to the time of day from real time clock 25, the fixed code and a biometric correlation factor, generating an encrypted security token. Such an encryption module is described in U.S. Pat. No. 4,819,267 and U.S. Pat. No. 4,405,829, the complete disclosures of both patents hereby being incorporated herein by reference. The security token is output to display 20. In this embodiment, the host system 10 includes a decryption module, capable of decrypting the encrypted code generated by the encryption module of biometric security apparatus 14. The capability to decrypt the token at the host system allows the token input by the user to be broken down into its biometric, time-varying and fixed code components. In some applications, this has distinct advantages over systems which are capable only of comparing the input token to a stored or time-generated value).

As to claim 9, Gullman fails to teach an authentication system comprising: a register including a login authentication data input part to input a login authentication data of an authenticatee and a login authentication data output part to output the login authentication data;

However, Takizawa discloses an authentication system comprising: a register including a login authentication data input part to input a login authentication data of an authenticatee and a login authentication data output part to output the login authentication data (Takizawa Figure 1 and column 5, paragraph 0021: The electronic payment system according to the present invention comprises an iris registration device...);

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that it would be necessary to have the ability to input and output the information the user registered (Takizawa Figure 1 and column 5, paragraph 0021: The electronic payment system according to the present invention comprises an iris registration device...).

The modified Gullman discloses an authenticator including an authentication data input part, data I/O part to input/output a certain data (Gullman column 4, lines 40-45: ... The apparatus 14 includes a power source 15, on/off switch 16, biometric sensor 18, display 20, processor 22 with on-chip random access memory, biometric input section 33 for receiving biometric information from the biometric sensor a read only memory...), and a processor to perform a predetermined processing using the authentication data (Gullman column 2, lines 53-57: ... Upon entry of the cardholder's biometric information, the processor executes the verification algorithm. The verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN, embedded serial number, account number...)). The modified Gullman fails to teach a server including a data input part to input an identification data of the authenticatee from the authenticator and to input the login authentication data from the register, a storage to store the login authentication data and an authentication processor to perform a predetermined authentication processing.

However, Takizawa discloses a server including a data input part to input an identification data of the authenticatee from the authenticator and to input the login authentication data from the register, a storage to store the login authentication data and an authentication processor to perform a predetermined authentication processing (Takizawa column 7, paragraph 0051-0053: In Step 4, iris data read by the iris authentication device 101 is

entered. By operating the personal computer of the iris registration device 110, personal information is also entered, such as the address, name, date of birth of the registered person of iris data. In Step 5, iris data and other information, which have been registered, are transferred to the iris certificate authority 120. The transferred data is stored in the database 122 in the iris certificate authority 120).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that an authentication system would need the ability to input and store authentication data (Takizawa column 7, paragraph 0051-0053: In Step 4, iris data read by the iris authentication device 101 is entered. By operating the personal computer of the iris registration device 110, personal information is also entered, such as the address, name, date of birth of the registered person of iris data. In Step 5, iris data and other information, which have been registered, are transferred to the iris certificate authority 120. The transferred data is stored in the database 122 in the iris certificate authority 120).

The further modified Gullman discloses a credit appraiser to appraise a credit of the authenticatee using the identification data (Gullman column 4, lines 13-36: The access device 12 sends the token to the host 10 which decodes the token to identify the embedded fixed code and correlation factor. In an alternative embodiment, the security apparatus 14 is coupled directly to the host system 10, such that the token output is transmitted directly to the host without the need for displaying the token or manual entry by the user. The coupling can be accomplished using, for example, standard data communication cable or any other known data transmission technique. To properly decode the token, the security apparatus 14 is synchronized with the host system 10 so that the time varying code is identical at both the security mechanism 14 and the

host system 10. In the challenge code embodiment, the host system, having generated the challenge code, retains the challenge code in memory to decode the token. The host 10 identifies the user with the fixed code and verifies the identification based on the correlation factor. The host system 10 permits full or limited entry based upon the level of authorization assigned to a given user (as identified by the fixed code). For example, a given user may be allowed to perform an electronic funds transfer only from a prescribed account); and a terminal including an appraisal result input part to input the appraisal result output from the server (Gullman column 3, lines 37-39: According to the invention, the biometric security mechanism 14 generates a security token which the user inputs to the access device). The further modified Gullman fails to teach wherein the authenticator reads the authentication processor input from the server into the processor to collate the authentication data of the authenticatee with the login authentication data by the authentication processor, then outputs the identification data of the authenticatee to the server when the authenticatee is authenticated as a user registered previously.

However, Takizawa discloses wherein the authenticator reads the authentication processor input from the server into the processor to collate the authentication data of the authenticatee with the login authentication data by the authentication processor, then outputs the identification data of the authenticatee to the server when the authenticatee is authenticated as a user registered previously (Takizawa column 6, paragraph 0029: An iris authentication device 120 is a biometric certificate authority that stores iris data of customers transmitted from the iris registration devices, and on receiving a request from a customer or the like, authenticates a customer by checking whether or not the customer is a very person registered in advance, based on iris data, and notifies a result by return).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that both systems are authenticating a user based on previous data stored and data currently being entered (Takizawa column 6, paragraph 0029: An iris authentication device 120 is a biometric certificate authority that stores iris data of customers transmitted from the iris registration devices, and on receiving a request from a customer or the like, authenticates a customer by checking whether or not the customer is a very person registered in advance, based on iris data, and notifies a result by return).

The further modified Gullman discloses the server appraises credit of the authenticatee in the credit appraiser to output a result of the appraisal to the terminal (Gullman column 4, lines 13-36: The access device 12 sends the token to the host 10 which decodes the token to identify the embedded fixed code and correlation factor. In an alternative embodiment, the security apparatus 14 is coupled directly to the host system 10, such that the token output is transmitted directly to the host without the need for displaying the token or manual entry by the user. The coupling can be accomplished using, for example, standard data communication cable or any other known data transmission technique. To properly decode the token, the security apparatus 14 is synchronized with the host system 10 so that the time varying code is identical at both the security mechanism 14 and the host system 10. In the challenge code embodiment, the host system, having generated the challenge code, retains the challenge code in memory to decode the token. The host 10 identifies the user with the fixed code and verifies the identification based on the correlation factor. The host system 10 permits full or limited entry based upon the level of authorization assigned to a given user (as identified by the fixed code). For example, a given user may be allowed to perform an electronic funds transfer only from a prescribed account).

As to claim 10, Gullman discloses an authenticator comprising: an image reader to input an image; an authentication data producer to produce an authentication data out of the image (Gullman column 5, lines 42-55: The biometric sensor 18 detects biometric input from a user (i.e., card-holder, pen-holder), the exact nature of which is not critical to the invention, so long as it senses information which is basically personal and substantially invariant in characteristics which are detected. According to various embodiments, the sensor 18 may detect a fingerprint, a signature, a voice or other like information. For the card embodiment 14', the sensor 18 may be a scanning device which detects a fingerprint or pressure sensing device which detects a signature. Alternatively, a CCD imaging device could be used to capture a picture of the fingerprint or signature. The sensor 18 also could be a voice detector). Gullman fails to teach a collator to collate the authentication data with another authentication data.

However, Takizawa discloses a collator to collate the authentication data with another authentication data (Takizawa column 8, paragraph 0055: ...The database contains the name, address, ID, iris data of each customer and his authentication code formed by adding an electric signature to the certificate....).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that in the database Takizawa is assembling i.e. collating the authentication data (Takizawa column 8, paragraph 0055: ...The database contains the name, address, ID, iris data of each customer and his authentication code formed by adding an electric signature to the certificate....).

The modified Gullman discloses a data input part to input a data including a login authentication data (Gullman column 4, lines 40-45: ... The apparatus 14 includes a power source 15, on/off switch 16, biometric sensor 18, display 20, processor 22 with on-chip random access memory, biometric input section 33 for receiving biometric information from the biometric sensor a read only memory...); and a processor to perform a predetermined processing using the data input from the data input part and the image (Gullman column 2, lines 53-57: ... Upon entry of the cardholder's biometric information, the processor executes the verification algorithm. The verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN, embedded serial number, account number...)), wherein the processor reads the authentication data producer and the collator from the data input part for the authentication data producer to produce the authentication data correspondent to the image (Gullman column 2, lines 40-47: According to another embodiment of the invention, the token is derived from the results of the above described biometric comparison, plus a user input challenge code from the host, rather than a time varying value. In a further embodiment, the biometric information is collected from the operation of the user of inputting the challenge to the device, either using a keypad, writing tablet or by voice...). Gullman fails to teach and the collator checks to compare the login authentication data with the authentication data correspondent to the image.

However, Takizawa discloses and the collator checks to compare the login authentication data with the authentication data correspondent to the image (Takizawa column 8, paragraph 0055: ...The database contains the name, address, ID, iris data of each customer and his authentication code formed by adding an electric signature to the certificate....).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that in the database Takizawa is assembling i.e. collating the authentication data (Takizawa column 8, paragraph 0055: ...The database contains the name, address, ID, iris data of each customer and his authentication code formed by adding an electric signature to the certificate....).

As to claim 11, the further modified Gullman discloses the authenticator of claim 10, wherein the login authentication data is encrypted; the data input part inputs a decrypter to decrypt the login authentication data; and the collator checks to compare the login authentication data decrypted by the decrypter with the authentication data correspondent to the image (Gullman column 5, lines 15-33: Alternatively, processor 20 may include a standard encryption module which applies an encryption algorithm to the time of day from real time clock 25, the fixed code and a biometric correlation factor, generating an encrypted security token. Such an encryption module is described in U.S. Pat. No. 4,819,267 and U.S. Pat. No. 4,405,829, the complete disclosures of both patents hereby being incorporated herein by reference. The security token is output to display 20. In this embodiment, the host system 10 includes a decryption module, capable of decrypting the encrypted code generated by the encryption module of biometric security apparatus 14. The capability to decrypt the token at the host system allows the token input by the user to be broken down into its biometric, time-varying and fixed code components. In some applications, this has distinct advantages over systems which are capable only of comparing the input token to a stored or time-generated value).

As to claim 12, the further modified Gullman discloses the authenticator of 10. The further modified Gullman fails to teach wherein the image is an eye-image of the authenticatee,

and the authentication data producer produces the authentication data according to an iris pattern of the eye-image of the authenticatee.

However, Takizawa discloses wherein the image is an eye-image of the authenticatee, and the authentication data producer produces the authentication data according to an iris pattern of the eye-image of the authenticatee (Takizawa abstract).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Gullman and Takizawa because Gullman teaches using biometric information to authenticate a user and Takizawa teaches using iris scanning (which is biometric information) to authenticate a user (Takizawa abstract, column 7, paragraph 0053: ...The transferred data is stored in the database in the iris certificate authority...and column 8, paragraph 0055: ...The database contains the name, address, ID, iris data of each customer and his authentication code formed by adding an electric signature to the certificate....).

As to claim 13, Gullman discloses a server comprising: a data input part to input data including an authentication data (Gullman column 4, lines 40-45: ... The apparatus 14 includes a power source 15, on/off switch 16, biometric sensor 18, display 20, processor 22 with on-chip random access memory, biometric input section 33 for receiving biometric information from the biometric sensor a read only memory...); an encrypter to encrypt the authentication data for a login authentication data(Gullman column 5, lines 15-33: Alternatively, processor 20 may include a standard encryption module which applies an encryption algorithm to the time of day from real time clock 25, the fixed code and a biometric correlation factor, generating an encrypted security token. Such an encryption module is described in U.S. Pat. No. 4,819,267 and

U.S. Pat. No. 4,405,829, the complete disclosures of both patents hereby being incorporated herein by reference. The security token is output to display 20. In this embodiment, the host system 10 includes a decryption module, capable of decrypting the encrypted code generated by the encryption module of biometric security apparatus 14. The capability to decrypt the token at the host system allows the token input by the user to be broken down into its biometric, time-varying and fixed code components. In some applications, this has distinct advantages over systems which are capable only of comparing the input token to a stored or time-generated value). Gullman fails to teach a storage to store the login authentication data; and a data output part to output data stored in the storage.

However, Takizawa discloses a storage to store the login authentication data; and a data output part to output data stored in the storage (Takizawa column 7, paragraph 0051-0053: In Step 4, iris data read by the iris authentication device 101 is entered. By operating the personal computer of the iris registration device 110, personal information is also entered, such as the address, name, date of birth of the registered person of iris data. In Step 5, iris data and other information, which have been registered, are transferred to the iris certificate authority 120. The transferred data is stored in the database 122 in the iris certificate authority 120).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that an authentication system would need the ability to input, to store, and to output authentication data (Takizawa column 7, paragraph 0051-0053: In Step 4, iris data read by the iris authentication device 101 is entered. By operating the personal computer of the iris registration device 110, personal information is also entered, such as the address, name, date of birth of the registered person of iris data. In Step 5, iris data and other information, which have

been registered, are transferred to the iris certificate authority 120. The transferred data is stored in the database 122 in the iris certificate authority 120).

As to claim 14, the modified Gullman discloses the server of claim 13. The modified Gullman fails to teach wherein the storage stores: an authentication data producer to produce an authentication data using an image, a collator to collate the authentication data with another authentication data, and.

However Takizawa discloses wherein the storage stores: an authentication data producer to produce an authentication data using an image (Takizawa abstract), a collator to collate the authentication data with another authentication data (Takizawa column 8, paragraph 0055: ...The database contains the name, address, ID, iris data of each customer and his authentication code formed by adding an electric signature to the certificate....), and

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Gullman and Takizawa because Gullman teaches using biometric information to authenticate a user and Takizawa teaches using iris scanning (which is biometric information) to authenticate a user (Takizawa abstract, column 7, paragraph 0053: ...The transferred data is stored in the database in the iris certificate authority...and column 8, paragraph 0055: ...The database contains the name, address, ID, iris data of each customer and his authentication code formed by adding an electric signature to the certificate....).

The further modified Gullman discloses a decrypter to decrypt the login authentication data (Gullman column 5, lines 15-33: Alternatively, processor 20 may include a standard encryption module which applies an encryption algorithm to the time of day from real time clock

25, the fixed code and a biometric correlation factor, generating an encrypted security token. Such an encryption module is described in U.S. Pat. No. 4,819,267 and U.S. Pat. No. 4,405,829, the complete disclosures of both patents hereby being incorporated herein by reference. The security token is output to display 20. In this embodiment, the host system 10 includes a decryption module, capable of decrypting the encrypted code generated by the encryption module of biometric security apparatus 14. The capability to decrypt the token at the host system allows the token input by the user to be broken down into its biometric, time-varying and fixed code components. In some applications, this has distinct advantages over systems which are capable only of comparing the input token to a stored or time-generated value).

As to claim 15, Gullman discloses a register comprising: an image reader to input an image of a user to be registered (Gullman column 5, lines 42-55: The biometric sensor 18 detects biometric input from a user (i.e., card-holder, pen-holder), the exact nature of which is not critical to the invention, so long as it senses information which is basically personal and substantially invariant in characteristics which are detected. According to various embodiments, the sensor 18 may detect a fingerprint, a signature, a voice or other like information. For the card embodiment 14', the sensor 18 may be a scanning device which detects a fingerprint or pressure sensing device which detects a signature. Alternatively, a CCD imaging device could be used to capture a picture of the fingerprint or signature. The sensor 18 also could be a voice detector). Gullman fails to teach an authentication data producer to produce a certain authentication data using the image.

However, Takizawa discloses an authentication data producer to produce a certain authentication data using the image (Takizawa abstract);

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that if the image was being used as authentication data then you would have to have a way to turn it into something useable (Takizawa abstract).

Gullman discloses an individual data input part to input an individual data of the user to be registered (Gullman column 4, lines 40-45: ... The apparatus 14 includes a power source 15, on/off switch 16, biometric sensor 18, display 20, processor 22 with on-chip random access memory, biometric input section 33 for receiving biometric information from the biometric sensor a read only memory...); and a data output part to output the authentication data and the individual data (Gullman column 2, lines 33-35: The mechanism verifies the input against the template, then generates and displays a token based on the verification).

As to claim 16, the modified Gullman discloses the register of claim 15. The modified Gullman fails to teach wherein the image is an eye-image of the user to be registered, and the authentication data producer produces the authentication data according to an iris pattern of the eye-image of the user to be registered.

However Takizawa discloses wherein the image is an eye-image of the user to be registered, and the authentication data producer produces the authentication data according to an iris pattern of the eye-image of the user to be registered (Takizawa abstract).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Gullman and Takizawa because Gullman teaches using biometric information to authenticate a user and Takizawa teaches using iris scanning (which is biometric information) to authenticate a user (Takizawa abstract, column 7, paragraph 0053: ...The

transferred data is stored in the database in the iris certificate authority...and column 8, paragraph 0055: ...The database contains the name, address, ID, iris data of each customer and his authentication code formed by adding an electric signature to the certificate....).

As to claim 17, Gullman discloses a terminal comprising: an appraisal result input part to input a credit appraisal of a user to purchase a product (Gullman column 3, lines 37-39: According to the invention, the biometric security mechanism 14 generates a security token which the user inputs to the access device). Gullman fails to teach and a data output part to output a data including a data showing whether or not the product is accepted to be purchased based on a result of the credit appraisal.

However, Takizawa discloses and a data output part to output a data including a data showing whether or not the product is accepted to be purchased based on a result of the credit appraisal (Takizawa Figure 11, Figure 14).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that if this authentication system was being used for purchasing products that somewhere the acceptance would be outputted to verify whether it was correct (Takizawa Figure 11, Figure 14).

As to claim 18, the modified Gullman discloses the terminal of claim 17. The modified Gullman fails to teach wherein the data output part outputs the data including the data showing whether or not the product is accepted to be purchased using an infrared ray.

However, Park discloses wherein the data output part outputs the data including the data showing whether or not the product is accepted to be purchased using an infrared ray (Park Figure 29).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that the transmission of data could be infrared (Park Figure 29).

As to claim 19, the modified Gullman discloses the authentication system of claim 7, wherein the server includes an encrypter to encrypt the authentication processor and the login authentication data by a predetermined encrypting method; stores a decrypter to decrypt encrypted the authentication processor and the login authentication data in the storage; and outputs the decrypter and encrypted the authentication processor and the login authentication data; and the authenticator decrypts the authentication processor and the login authentication data input into the data input part by the decrypter (Gullman column 5, lines 15-33: Alternatively, processor 20 may include a standard encryption module which applies an encryption algorithm to the time of day from real time clock 25, the fixed code and a biometric correlation factor, generating an encrypted security token. Such an encryption module is described in U.S. Pat. No. 4,819,267 and U.S. Pat. No. 4,405,829, the complete disclosures of both patents hereby being incorporated herein by reference. The security token is output to display 20. In this embodiment, the host system 10 includes a decryption module, capable of decrypting the encrypted code generated by the encryption module of biometric security apparatus 14. The capability to decrypt the token at the host system allows the token input by the user to be broken down into its biometric, time-varying and fixed code components. In some applications, this has distinct

advantages over systems which are capable only of comparing the input token to a stored or time-generated value).

As to claim 20, the further modified Gullman discloses the authenticator of claim 11. The further modified Gullman fails to teach wherein the image is an eye-image of the authenticatee, and the authentication data producer produces the authentication data according to an iris pattern of the eye-image of the authenticatee.

However Takizawa discloses wherein the image is an eye-image of the authenticatee, and the authentication data producer produces the authentication data according to an iris pattern of the eye-image of the authenticatee (Takizawa abstract).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Gullman and Takizawa because Gullman teaches using biometric information to authenticate a user and Takizawa teaches using iris scanning (which is biometric information) to authenticate a user (Takizawa abstract, column 7, paragraph 0053: ...The transferred data is stored in the database in the iris certificate authority...and column 8, paragraph 0055: ...The database contains the name, address, ID, iris data of each customer and his authentication code formed by adding an electric signature to the certificate....).

Prior Art

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 6987870 is pertinent because it teaches ...the personal identification data can be

biometric data such as retina images, voice audio, and fingerprints, or a smart card. The method typically comprises: establishing a network with a plurality of connecting destination addresses... creating a library where a plurality of biometric data items associated with a particular user, are cross-referenced to destination addresses; accessing the library; searching the library for biometric data matching the supplied biometric data; and, selecting the destination address corresponding to the matching biometric data. US 6483930 is pertinent because it teaches a compact, handheld imaging apparatus which can be used to capture high-quality iris images for identification of a person... template of the image is then compared to a database of previously stored templates of images to identify the person. US 6016476 is pertinent because it teaches ...the PDA includes a modem, a serial port and/or a parallel port so as to provide direct communication capability with peripheral devices (such as POS and ATM terminals) and is capable of transmitting or receiving information through wireless communications such as radio frequency (RF) and infrared (IR) communication.... Upon biometric verification, the Universal Card is written with the selected card information, which is then used to initiate a consumer transaction. US 5892900 is pertinent because it teaches the present invention provides systems and methods for electronic commerce including secure transaction management and electronic rights protection. Electronic appliances such as computers employed in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Rebecca L. Pachura whose telephone number is (571) 270-3402. The examiner can normally be reached on Monday-Thursday 7:30 am-6:00 pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.\

/R. L. P./
Examiner, Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/25/08